ATRC
ARIZONA
TRANSPORTATION
RESEARCH
CENTER

RESEARCH NOTES:

Project 502(2)

February 2002

ADOT USES FOR VIRTUAL PRIVATE NETWORKING TECHNOLOGY: PHASE 2 – FINAL TEST REPORT

Highlights

- VPN technology is suitable for remote access by employees and for LAN-to-LAN connectivity to other government agencies with a need for high-volume processing and retrieval of ADOT records.
- The system should be deployed in a full roll-out and fully integrated into ADOT's production network.
- ADOT should consider using the VPN to further expand connectivity into 3rd party processing offices for MVD.

Background

The goal of this study is to determine the effectiveness, appropriateness of the security, and potential cost reductions that have proven themselves when Virtual Private Networking technology and services are in use.

ADOT network security policies prohibit direct connections with outside constituents unless a VPN is used. The ADOT network did not provide the sufficient level of firewall security desired but ADOT network administrators and managers began to explore some options using the technology with internal trials and vendor-supplied trial equipment. Discussions ensued about the varied landscape of VPNs and ADOT's readiness to adopt leading-edge systems in light of a technology that reinvents itself on a near daily basis.

ADOT customers are faced with soaring communications costs. External customers such as MVD Third Parties and other Government entities access the ADOT network by either dialing in or paying local telecommunications carriers for dedicated lines. All customers that are located outside of the Phoenix metro area must incur long distance charges to connects to the ADOT network. This may impede potential customers from providing ADOT services or doing ADOT business. Due to Lata and facilities restriction telecomm carriers cannot always provide service to remote locations. ADOT customers that travel frequently and must connect to the ADOT network are incurring excessive long distance charges.

The solution should provide a reliable and secure connection to ADOT network using low cost public networks. This solution should support internal and external customers that have a business need. This project will analyze and test industry standards of VPN technology to determine best the solution for ADOT.

Approach

Employees in the ADOT ITG Department initiated evaluation and testing VPN technology early in the first phase of this project using equipment and software that ADOT already owned. The intent was for ITG to make a recommendation to ADOT for a system was deemed both reliable and secure. Two systems were tested:

1. Microsoft Windows
2. Checkpoint VPN1

Due to ADOT's commitment to the Microsoft product line for both infrastructure (networks and OSs) and application programs (terminal server, Outlook, etc.), using VPNs other than Microsoft's was thought to lead to support and reliability problems. Marketplace research supports this theory. Since many of the protocols used within the Microsoft family of products are atypical of the protocols most often found on the Intern4t. The support that vendors other than Microsoft are providing on their VPN products often do not work will with Microsoft protocols, but this will not always be the case. As VPN technology matures and standards shake themselves out, in the future VPN products should become fungible. however in today's marketplace reality they're not quite there yet and organizations simply cannot wait.

As a participant in the standards process, Microsoft pledges support on future products for whatever the industry standard calls for and has provided a migration path for users. Despite the criticisms of Microsoft's implementation of PPTP, what's important is that the system does operate as needed and still provides the sufficient layer of security needed to protect MVD records.

Beginning in August 2000, ADOT business partners began recruiting efforts to locate potential testing organizations with an understanding that they were participating in an experiment. Once the paperwork found its way back to ITG with the appropriate approvals, 5 organizations were participants

- City of Phoenix
- Federal Bureau of Investigations
- Scottsdale Police Department
- RRRobertson Investigations
- Kolb, Stewart & Associates Investigations

The VPN field-testing that took place from August 2000 through October 2001 for both types of access to the ADOT VPN – server-to-server and remote client to server – showed great promise and indicated that VPNs should be made an ADOT offering for a wider audience of potential users.

Findings

At the end of the testing period, 72 people were set-up to use the VPN for remote access and for LAN-to-LAN connectivity within the Phoenix Prosecutors Office. In September 2001, an online survey was developed by the research and sent out to the user base of 72 people. A number of questions related to system configurations from remote access workstations and usability questions were asked using the Likert scale (e.g. 1-easy, 3-moderate, 5-difficult) for developing survey questions. The surveying period was open for two weeks and survey recipients were request to complete the survey two times, but only 22 responses were eventually received

Below are some selected comments and recommendations forms the survey forms received.

- "I hope you intend to take it to the next state (CryptoCare authentication or ??). If possible, it should be opened up, especially to those who telecommute on a regular basis."

- "It is wonderful and normally a very reliable connections"

- "Worked very nicely with a High Speed Wireless Modem. Even a Slow Connection was not too bad, for critical times I need access to files."

- "Wonderful. I sue it often; when I telecommute on Thursday & at other times. It's useful in that I have access to all my files on the network regardless of where I'm working."

- I have been using the VPN since approximately March 20012. The reliability of the system is outstanding. I think there have only been two/three times when my connections was dropped. I was able to log back in right away."

- Faster than speeding bullet.

- Very convenient and useful, lived the flexibility when I didn't have to dial in, like not having my phone line tied up."

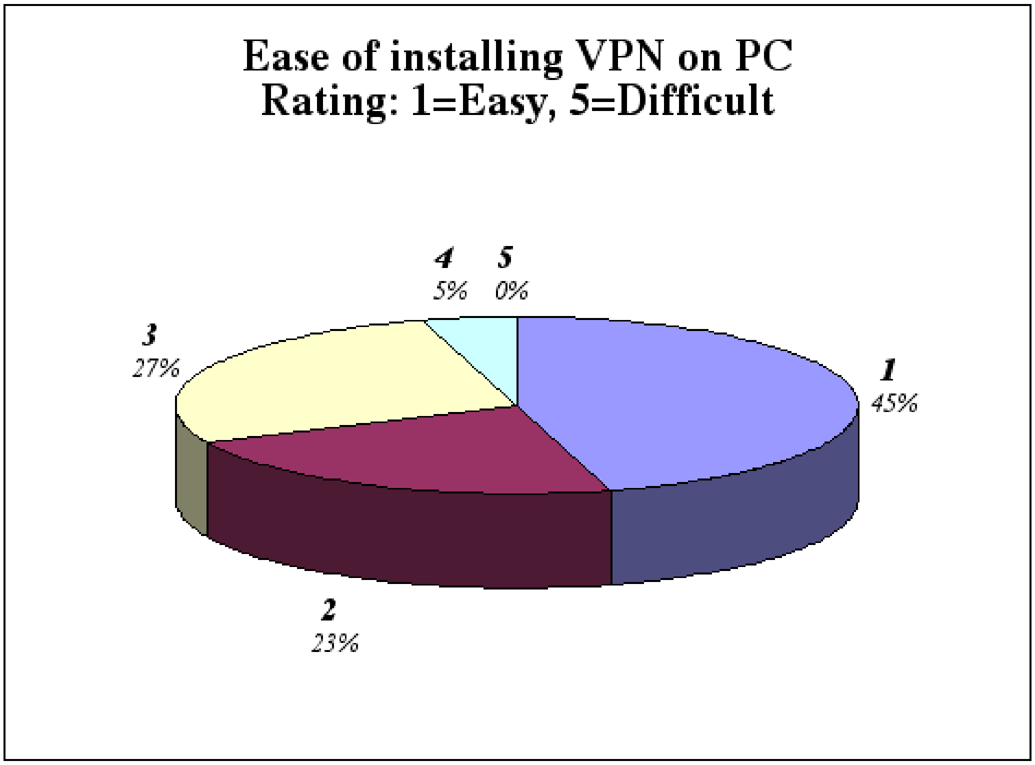
- I absolutely LOVE it! Makes my job so much easier and I'm more efficie**nt.**

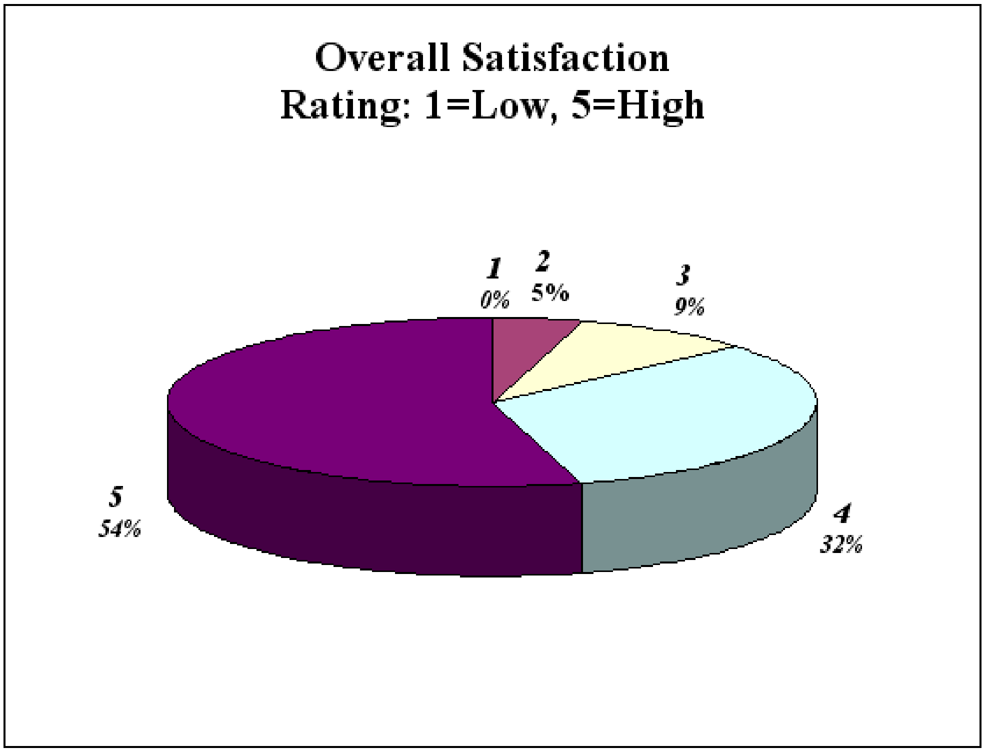
Conclusions

ADOT's system has proven that VPN technology is suitable for remote access by employees and for LAN-to-LAN connectivity to other government agencies with a need for high-volume processing and retrieval of ADOT records.

The system should be deployed in a full roll-out once a solution that's compatible with ADOT's two-factor authentication mechanisms is in place and fully integrated into ADOT's production network.

ADOT should also consider using the VPN to further expand connectivity into 3rd party processing offices for MVD.





The full report *ADOT Uses for Virtual Private Networking Technology: Phase 1 – Pre-Pilot Test Report* by Mark Merkow (Arizona Department of Transportation, report number FHWA-AZ-01-502(1), published February 2001) is available from the Arizona Transportation Research Center, 206 S. 17 Ave., mail drop 075R, Phoenix, AZ 85007; phone 602-712-3138.